REMARKS

Reconsideration of this Application is respectfully requested. Upon entry of the foregoing amendments, claims 1, 3-6, 9-11, 13-16, and 19-21 are pending in the application, with claims 1 and 11 being the independent claims. Claims 2, 7-8, 12, 17-18, and 22 have been canceled without prejudice or disclaimer. Support for the subject matter of the amended claims is contained in the application as originally filed. Because the foregoing changes introduce no new matter, their entry is respectfully requested.

Based on the above Amendment and the following Remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 112

The Examiner has rejected claims 1, 3-6, 9-11, 13-16, and 19-21 under 35 U.S.C. §112, second paragraph as being indefinite. Applicant respectfully submits that the rejection of claims 1, 3-6, 9-11, 13-16, and 19-21 are overcome by the accompanying amendment thereto. In particular, Applicant has incorporated the amendments suggested by the Examiner and further amended claims 1 and 11 to more particularly describe the present invention.

The Examiner contends that the specification fails to describe how "unchanged key information" is restored if key information changed by the virus is extracted. *See* Office Action, pg. 2, ¶ 5, lines 5-8. In response, Applicant notes that claims 1 and 11 have been amended to recite "modified key information." Applicant further directs the Examiner's attention to paragraphs 18 and 50-55 and FIGs. 2A-2C as originally filed. Paragraph 53, in particular, describes the calculation for determining what modifications were made by the virus and thus will be reversed to clean the host. As shown and described, the necessary information can be obtained about the virus such that the key information may subsequently be restored by conventional methods such as those described in paragraph 57.

The Examiner further contends that the specification fails to adequately describe from where and to where the "unchanged key information" is restored. In response, Applicant directs the Examiner's attention to the discussion on pages 15 and 18-19 of the specification. The host body is restored from its modified state to its unmodified state using the information obtained. As described, the system may write the clean file to the same location or another location as understood by one skilled in the art.

Applicant respectfully traverses the Examiner's rejection of claim 1, 3-6, 9-11, 13-16, and 19-21.

Rejections under 35 U.S.C. § 103

Claims 1, 3-6, 9-11, 13-16, and 19-21

The Examiner has rejected claims 1, 3-6, 9-11, 13-16, and 19-21 under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 5,842,002 to Schnurer et al. ("Schnurer") and U.S. Patent No 5,485,575 to Chess et al. ("Chess"). Schnurer and Chess, taken individually or combined fail to teach or suggest the method of the present invention including, *inter alia*, (1) simulating in a virtual computer circumstance, (2) providing a plurality of objects to be scanned, (3) comparing the plurality of objects, and (4) cleaning the virus from the infected target object, as is called for by amended claim 1. Independent claim 11 is directed to a computer system and includes similar features as claim 1. For example, claim 1 calls for

> A method for detecting and cleaning computer viruses, comprising the steps of:
>
> simulating in a computer a *virtual* computer circumstance, wherein computer viruses will reside on the virtual computer circumstance;
>
> providing a *plurality* of objects to be infected by computer viruses that induce virus infection;
>
> loading a target object to be scanned into said simulated virtual computer circumstance, said target object being a host possibly attached by a virus;

activating any virus attached on the target object to be scanned in said simulated virtual computer circumstance to induce virus infection of the plurality of objects and *generating standard samples* which have been infected, wherein if a virus is attached to the target object and the virus is activated, the target object will include a host body and a virus body;

comparing the plurality of objects after processing in the activating step with the plurality of objects to be infected originally provided and determining whether there is any change or not, if there is a change, the target object to be scanned contains a virus, otherwise the target object to be scanned is free of viruses;

analyzing the generated standard samples and extracting information on the viruses indicated by changes between the plurality of objects before infection and the standard samples after infection when it is determined that said target object to be scanned contains a virus, *said information including at least the size of the virus and key information of the host which has been changed by the virus*; and

cleaning the virus from the infected target object by locating the host body and the virus body in the target object after the activation step, restoring modified key information of the host on the basis of said information, and removing the virus body from the target object after the activation step according to the virus size. (emphasis added)

As the Examiner admits, Schnurer further fails to disclose or suggest the analyzing step of the present invention. *See* Office Action, ¶ 5, lines 16 et seq. Instead, Schnurer discloses "watching" emulations to determine if a virus exists. *See* col. 4, lines 58-59. While the body is trapped in the emulation chamber, activity with other files and components is "monitored" to indicate if a virus exists. *See* col. 8, lines 13-20. After detection, everything in the emulation chamber is immediately eliminated, not analyzed. *See* FIG. 6C and col. 8, line 31.

In contrast, the method of the present invention involves "analyzing the generated standard samples and extracting information on the viruses indicated by changes between the plurality of objects before infection and the standard samples after infection" after a virus has been detected. By analyzing the activity and changes *after* detection, the program can acquire information about the virus, which in turn can be applied to *clean* the virus from the infected

target. *See* Specification, pg. 6, ¶ 15. In essence, the information is analyzed in addition to being monitored to aid in adaptive, real-time cleaning. *See* Specification, pg. 15, ¶ 43.

Additionally, Schnurer does not disclose cleaning the virus from the target body as called for by claims 1 and 11. Instead, Schnurer discloses a method for detecting a virus, trapping the virus in an emulation chamber 48, and then clearing the emulation chamber. *See* Abstract and FIG. 6C. Upon detection, the *entire* object including a host body is deleted. *See* col. 8, line 31. In contrast, claims 1 calls for cleaning whereby the virus body is removed and the host body is restored. *See* Specification, ¶¶ 43-44.

Chess likewise fails to disclose or suggest the method of the present invention including simulating in a virtual computer circumstance and loading the target body into the virtual computer. Instead, Chess discloses obtaining pairs of original, uninfected host files and the same programs after viral infection to facilitate anti-virus scanning and repair. The files and objects reside in and are activated in a *real* computer environment. *See* col. 4, lines 31-32 and col. 3, lines 25-33. Thus, the step of obtaining pairs of objects (host and infected host) may in fact destroy or caused unpredicted damages to the computer running the program. In other words, the method of extracting repair information in accordance with Chess is not safe. In contrast, the present invention safeguards the computer by locating the bodies in *virtual* computer circumstance.

Chess further fails to disclose the cleaning step of the present invention. Instead, Chess discloses extracting information to enable anti-virus software to complete the repair of an infected file by obtaining pairs of original, uninfected host files and the same programs after viral infection. *See* col. 4, lines 31-53. In a conventional manner, the extracted information is stored for improved scanning in the future. In one embodiment, the results of the virus analysis are "incorporated manually or automatically into databases used by anti-virus software" for future releases. *See* col. 3, lines 25-28. In another embodiment, the analysis itself is "incorproated into anti-virus software that runs on individual computers or networks" and updated automatically. *See* col. 3, lines 29-33.

Whereas Chess is directed to scanning a computer for viruses, the present invention is directed to detecting and cleaning in a virtual circumstance. The present invention involves removing the virus body from the target body and restoring or repairing modified key information in the host. Storing repair information in a database in accordance with Chess is different than repairing the object immedately. By repairing the object immediately, the object can be released from the virtual computer circumstance without consequence to the computer environment. Damage to the real computer and its operation is further minimized.

In fact, Chess teaches away from the present invention because the object is allowed to enter the real computer environment. Chess is directed to a reactionary method for virus protection involving scanning a real computer for viruses and thereafter resolving damage done by the viruses by utilizing the information it has learned about the virus. In comparison, the present invention is directed towards preventing an infected body from ever reaching a real computer environment and cleaning in real-time.

Furthermore, there is no motivation to combine Schnurer and Chess. Schnurer teaches trapping and destroying the virus in an emulation chamber before it reaches the real computer environment. *See* Abstract. Chess is directed to scanning and eradicating viruses in a real computer environment. *See* col. 1, lines 19-24. Once the computer is scanned and the virus detected, the system taught by Chess seeks to reverse the effects of the virus. *See* Abstract. One would not be motivated nor able to combine the analysis of Chess with the trapping system of Schnurer because the system taught by Schnurer is intended to prevent virus bodies from ever reaching the computer. Thus, there would be no virus for which to scan using the system taught by Chess.

Even if one were to combine the teachings of Schnurer and Chess, one still would not arrive at the present invention because Schnurer does not disclose or suggest the comparison step of the present invention. Schnurer instead discloses trapping a virus in an emulation chamber 48 and fooling it into acting. *See* col. 7, lines 3-8. The system detects the presence of a virus by watching for changes to items other than the virus body itself. *See* col. 7, lines 48-52. Any attempted writes or changes to the IRQ table, FAT file, or other internal disks and likewise

indicates the presence of a virus. *See* col. 7, lines 53-67. The virus may also be detected by its signature or checks of internal components. *See* col. 8, lines 8-10 and 21-26.

In contrast, claim 1 calls for "comparing the plurality of objects after processing in the activating step with the plurality of objects to be infected originally provided and determining whether there is any change or not." In particular, the system watches for changes within the bodies themselves and compares the unmodified, originally-provided bodies with the generated sample of bodies after activation of any virus. If the objects after processing in the activating step are not the same as those originally provided, a virus is detected. Thus, the virus is detected by changes to the plurality of objects themselves rather than whether a single object in a closed environments attempts to access external components. Thus, the present invention identifies a virus "according to its 'result' instead of specific behaviors" as in Schnurer. *See* Specification, pg. 20, ¶ 58. The environment is used primarily to "bait" the virus in the present invention. In this manner, only a single group of objects must be monitored and the performance of detection and cleaning is increased.

For at least these reasons, Applicant respectfully submits that Schnurer and Chess, taken individually or combined, do not render obvious independent claims 1 and 11. Applicant submits that claims 3-6, 9-10, 13-16, and 19-21, which depend from claims 1 and 11, are allowable over the cited art for at least the same reasons noted above.

CONCLUSION

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided below.

PATENT

Attorney Docket No. A-70915/DJB/VEJ
Attorney Matter No. 469164-00005
Application No. 09/963,359

The Commissioner is hereby authorized to charge any underpayment of fees associated with this communication, including any necessary fees for extension of time or additional claims, and/or credit any overpayment to Deposit Account No. 50-2319 (Order No. 469164-00005; Docket No. A-70358/DJB/VEJ).

Prompt and favorable consideration of this Amendment and Response is respectfully requested.

Respectfully submitted,

DORSEY & WHITNEY LLP

Date: November 20, 2006

By: _____
Victor E. Johnson, Reg. No. 41,546

DORSEY & WHITNEY LLP
Suite 1000
555 California Street
San Francisco, California 94104-1513
Telephone: (415) 781-1989 Facsimile: (415) 398-3249